AIR COMMAND AND STAFF COLLEGE

DISTANCE LEARNING

AIR UNIVERSITY

CITIZEN 'CYBER' AIRMEN:

MAINTAINING READY AND PROFICIENT CYBERSPACE OPERATORS IN THE RESERVE COMPONENTS

by

Cyrus R. Champagne, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Proposal Advisor: Dr. Paul Moscarelli

Project Advisor: Dr. Gregory F. Intoccia

Maxwell Air Force Base, Alabama

February 2016

DISCLAIMER

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

TABLE OF CONTENTS

LIST OF FIGURES

ABSTRACT

The Department of Defense (DOD) steadily works to meet the U.S. government's increasing demand for cyberspace defense and cybersecurity with a strategy of objectives to defend its network of critical infrastructure against its adversaries. Of the strategy of objectives, the Reserve Components (RC) have been levied as a resource for expertise and to foster creative solutions to cybersecurity problems.

The purpose of the paper is to help improve the Air Force's strategy to recruit, train, and retain highly qualified cyberspace operations personnel in the RCs. The paper employs an evaluation methodology in order to determine whether current Air Force training methodologies are sufficient enough to maintain proficient and ready RC personnel for DOD's cyber defense posture. Among its key findings are challenges in recruiting and retaining highly trained and qualified personnel to serve in the Air Force RCs; current proficiency training requirements that require a considerable amount of time to complete, and the civilian life, military work imbalance for RC cyber personnel. Its key recommendations include offering similar incentives to RC cyber personnel just like ones offered to Active Duty personnel and Air Force pilots, provide flexible training schedules, short-duration activations, and leveraging civilian educational institutions for maintaining training requirements.

INTRODUCTION

The Department of Defense (DOD) is relying heavily on the Air Force Reserve Components (RCs) more so now than in the past 20 years to meet operational requirements and augment Active Duty (AD) forces. The Cyber Command and the military services continually identify gaps that need to be addressed in individual and collective training through frequent discussions with subject matter experts throughout DOD and military services. Current cyberspace personnel plus-up strategies assume that the Air Force RCs contain highly skilled technical personnel that will be able to train their personnel in timely manner and assist with conducting operations seamlessly. However, the Air Force RCs generally have a very limited training schedule – between generally 39-180 days annually, which requires Air Force RC personnel to accomplish their training requirements in only a fraction of the time as Air Force Active Component (AC) personnel for the year.

Handling Cyberspace operational duties require a significant level of training and costs related to such training, posing a challenge to fit within Air Force RC scheduling constraints. Air Force RC personnel are required to have proficiency training in the fundamentals of computer systems, operating systems, software applications and architecture, protocols, addressing and hardware.

Other hurdles persist, making it a challenge for the Air Force RC to assume a more active role in the Air Force cyber mission. The Air Force RCs face a tightly constrained budget. The cyberspace defense operational budget is exponentially expanding due to the increasing number of cyber threats each year and training dollars for cyberspace personnel are simultaneously increasing.

Recruitment and retention of cyberspace personnel for Air Force RCs needs a bolster. One challenge that the Air Force faces with recruiting and retaining the right personnel is the current budgetary constraints. For over a decade of extended combat operations, recruitment and retention for personnel within the Air Force remains at an all-time high. While this is a testament to the selfless service of members of the Air Force family, they are now faced with some very difficult financial choices that force the Air Force to reduce its overall size.

With all of these obstacles, this leaves an important question for the Air Force to answer. How can the Air Force RCs best overcome current training, recruiting, retention, surge demand, and work-life balance obstacles to meet the readiness and proficiency requirements of its cyberspace operations career field professionals?

To best meet the readiness and proficiency of Air Force RC personnel, the Air Force should transition cyberspace mission areas such as cyberspace support and cyberspace defense missions to Air Force RC units in the event that the commercial sector's standards do not meet future cyber defense requirements in time. In order to develop highly skilled professionals with cyberspace expertise, the Air Force should allow cyber personnel to accomplish online training from home while incentivizing with points toward retirement. In addition, the Air Force should redefine their budget strategy for Air Force RC personnel in cyberspace operations for cost-effective utilization. Furthermore, appropriate the cost savings realized from utilizing Air Force RC personnel to incentive pay as a way to recruit and retain civilian expertise, to cover the costs of personnel maintaining certifications requiring yearly renewal and upgrade training. Lastly, the Air Force should consider short-duration activations for Air Force RC cyber personnel to meet surge demands for cyberspace defense and keep a healthy work-life balance for the personnel.

Recruitment and retention of cyber personnel from the RCs represent a huge treasure in the Pentagon's development of a cyber force.[1] Offering incentives such as special duty assignment pay, assignment incentive pay and bonuses for Air Force RC personnel serving in operational cyber assignments will be the key to meet targeted recruiting and retention goals. Incentivizing is also a way to attracting a civilian workforce that is highly-skilled and fully qualified in cyberspace.

Most educational institutions in the civilian arena have already merged with commercial industry to provide training courses that maintains current and up-to-date technological advances. Due to the growing interest in cybersecurity, several large defense contractors such as Northrop Grumman, Lockheed Martin, Raytheon, and MITRE are offering variations on their internal training curriculum to DOD.

The work-life balance of traditional Reservists alone lends itself for DOD to explore alternative training methodologies that will allow Air Force RC personnel the opportunities for adhering to training guidelines to maintain their technical proficiency as well as meet surge demands. Providing these cyber Airmen with a support system that is tailored to the Air Force RCs and their families, as well as understanding how the Air Force RCs operate on a daily basis, will be key factors in assessing how Air Force RCs can meet DOD's operational demands.

This research paper explains how cybersecurity and cyberspace operations are viewed within DOD's cyber defense posture. This research paper provides an extensive background on the initial and continuous training requirements for personnel in the cyberspace operations to give the reader a basic understanding of the cyberspace career field. A background on the cyber mission force (CMF) requirements being levied on RC personnel and the cyber mission strategy set forth by USCYBERCOM and DOD to leverage RCs in expanding the national cyber defense

is also provided. Past years and future years budget proposals are given to show the overall impact of cybersecurity to the defense budget.

An in-depth analysis is conducted on the training requirements of Air Force cyberspace personnel requiring additional formal education or certifications that becomes the MAJCOM's or unit leadership's responsibility for ensuring compliance. An analysis of the challenges the Air Force RCs face in personnel recruitment and retention was conducted. The challenges associated with maintaining the work-life balance of Reserve personnel were analyzed along with possible concerns Air Force RCs may have with civilian employers. An analysis of budgetary requirements is conducted to determine if cost-effective strategies are in place to sustain Air Force RC personnel in maintaining their readiness and proficiency. This research paper also analyzes the challenges, problems, and key issues that Air Force RCs have to address as new and emerging technology develops in the cyberspace domain.

Following the above methodology, the paper recommends strategies that include assigning mission sets to Air Force RCs to conduct full-time cyber operations; leveraging acquired skillsets of Air Force cyberspace personnel from their civilian technical jobs, and budgeting appropriations for incentive pay to cyberspace personnel as a result of realized cost savings of Air Force RC utilization.

BACKGROUND AND SIGNIFICANCE

Cybersecurity and Cyberspace Operations within DOD

Cybersecurity has become a major hot topic of discussion throughout the duration of the Obama Administration. From the beginning of his Administration, the President made it clear that cybersecurity is one of the most important challenges that the U.S. faces as a nation. For cyber personnel, this means having the ability to implement proper cybersecurity awareness and

protections as well as enhancing capabilities to reduce cyber-vulnerabilities in the near- and long-terms through the use of cyber technology.[2]

DOD has placed high-level emphasis on the development of cyber forces to strengthen its cyber defense and cyber deterrence with the use of the most secure, reliable, and up-to-date technology that industry has to offer. DOD has vested a great deal of resources to have the technological and military advantage over its adversaries.

Many of DOD's critical functions and operations rely on commercial assets, including Internet service providers and global supply chains, over which DOD has no direct authority to mitigate risk effectively. The global technology supply chain affects mission critical aspects of the DOD enterprise and IT risks must be mitigated through strategic public-private sector cooperation.[3] Given the technical requirements and management responsibilities that cyber personnel are required to possess and understand to conduct CO and cybersecurity, it is important to understand the aspects of how cyber technology is integrated within the U.S. military environment.

Cybersecurity involves practicing standards and processes which help protect networks, computers, systems and information from attack, damage or unauthorized access. Cybersecurity also encompasses a body of technologies to protect information and systems from major cyber threats, such as cyber terrorism, cyber warfare, and cyber espionage.[4] The primary use of cyber technology in U.S. military cyber missions is to defend DOD networks, systems, and information, defend the U.S. homeland and U.S. national interests against cyberattacks of significant consequence, and provide cyber support to military operational and contingency plans.[5]

CO are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. CO are composed of the military, intelligence, and ordinary business operations of DOD in and through cyberspace. Cyberspace, while a global domain within the information environment, is one of five interdependent domains, the others being the physical domains of air, land, maritime, and space. Much as air operations rely on air bases or ships in the land and maritime domains, CO rely on an interdependent network of IT infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers, and the content that flows across and through these components. CO rely on links and nodes that reside in the physical domains and perform functions experienced both in cyberspace and the physical domains.[6]

Cyberspace can be described in terms of three layers: physical network, logical network, and cyber-persona (Figure 1). Each of the layers represent a level on which CO may be conducted.

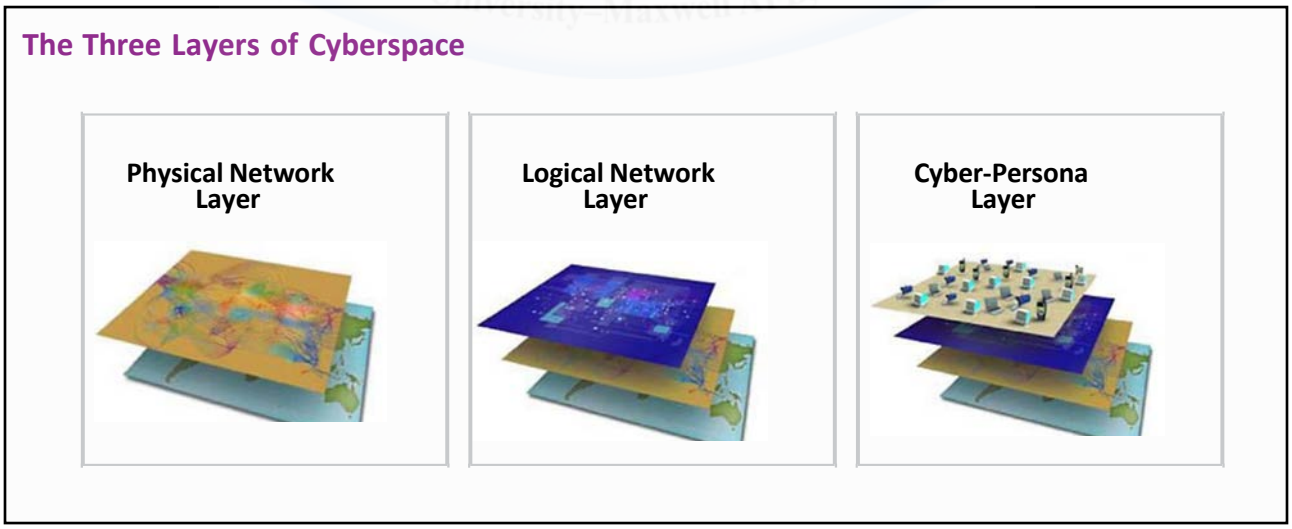

Figure 1. The Three Layers of Cyberspace[7]

The physical layer of cyberspace is comprised of the geographic component and the physical network components. It is the medium where the data travel. The geographic component is the location in land, air, sea, or space where elements of the network reside. While geopolitical boundaries can easily be crossed in cyberspace at a rate approaching the speed of light, there are still sovereignty issues tied to the physical domains. The physical network component is comprised of the hardware, systems software, and infrastructure (wired, wireless, cabled links, electromagnetic spectrum (EMS) links, satellite, and optical) that supports the network and the physical connectors (wires, cables, radio frequency, routers, switches, servers, and computers). However, the physical network layer uses logical constructs as the primary method of security (e.g., information assurance [IA]) and integrity (e.g., virtual private networks that tunnel through cyberspace). This is a primary target for signals intelligence (SIGINT), including computer network exploitation (CNE), measurement and signature intelligence, open source intelligence, and human intelligence. It is the first point of reference for determining jurisdiction and application of authorities. It is also the primary layer for geospatial intelligence, which can also contribute useful targeting data in cyberspace.[8]

The logical network layer consists of those elements of the network that are related to one another in a way that is abstracted from the physical network, i.e., the form or relationships are not tied to an individual, specific path, or node. A simple example is any web site that is hosted on servers in multiple physical locations where all content can be accessed through a single uniform resource locator (URL). For example, Defense Knowledge Online exists on multiple servers in multiple locations in the physical domains, but is represented as a single URL on the World Wide Web. A more complex example of the logical layer is the DOD's Nonsecure Internet Protocol Router Network (NIPRNET).[9]

The cyber-persona layer represents yet a higher level of abstraction of the logical network in cyberspace; it uses the rules that apply in the logical network layer to develop a digital representation of an individual or entity identity in cyberspace. The cyber-persona layer consists of the people actually on the network. Cyber-personas may relate directly to an actual person or entity, incorporating some biographical or corporate. Figure 1. The Three Layers of Cyberspace, The Three Layers of Cyberspace Physical Network Layer, Logical Network Layer, Cyber-Persona Layer Chapter I I-4 JP 3-12 data, e-mail and IP address(es), Web pages, phone numbers, etc. However, one individual may have multiple cyber-persona, which may vary in the degree to which they are factually accurate. A single cyber-persona can have multiple users. Consequently, attributing responsibility and targeting in cyberspace is difficult. Because cyber-personas can be complex, with elements in many virtual locations, but normally not linked to a single physical location or form, significant intelligence collection and analysis capabilities are required for the joint forces to gain sufficient insight and situational awareness (SA) of a cyber-persona to enable effective targeting and creation of the Joint Force Commander's (JFC's) desired effect.[10]

Training Requirements for Cyberspace Operations Personnel

DOD has developed a four-phase training model to assist the military services in implementing common individual and collective training standards for the CMF. The training model is composed of feeder courses that help military personnel obtain military occupation specialties for their respective services, foundation training built around specific CMF work categories, collective training for mission-oriented teams, and sustainment that keeps personnel abreast of changing needs and requirements. Initial cyber training typically lasts several months, but advanced cyber training required to work in joint operational environments typically requires several additional months of training.[11]

The 24th Air Force, also known as AFCYBER, under Air Force Space Command, was established to enable cross-domain synergy, while aligning common technical expertise, to present Air Force cyber force to the joint fight. In addition to standing up the 24th Air Force, the Air Force established the 17D Cyberspace Operator career field, a six-month long Undergraduate Cyber Training (UCT) was established and is in operation at Keesler Air Force Base. The training begins with a 23-week undergraduate cyber training course for officers and a 17-week cyber defense operations course for enlisted personnel. Airmen take a set block of classes such as mobile, space and satellite networking, cyber network threats and defense, cyber operations and information technology fundamentals, and even classes on laws and ethics practices.[12]

As of fiscal 2013, the graduation rate for those going through the officer undergraduate cyber training course is 92.5 percent; and for enlisted Airmen in the cyberspace defense operator training course, 88 percent, according to Air Education and Training Command's 333rd Training Squadron Public Affairs office.[13]

For some Airmen, that first phase of training may be enough to land them their first assignment. Those going through undergraduate and/or cyber defense training "are also just personnel members who are going to work for the Air Force either at an assigned base ... or in some sort of cyber-related role. Airmen are trained to a "joint standard" so they can be assigned to Air Force-specific or joint missions. Airmen expected to be part of the USCYBERCOM teams must take an additional nine-week intermediate network warfare training course at Hurlburt Field, Fla. That phase provides more hands-on training.[14]

The Air Force has put more than 11,500 enlisted Airmen and officers through cyber-related training since 2011. In 2013, for example, 20 percent more Airmen trained for 3D1X2 than the previous year. Overall, 300 more Airmen were trained in nine cyber-related enlisted

specialties in 2013 than in 2012. Training for the 17D cyberspace operations officers climbed 28 percent in 2013.[15]

Cyber 200 and 300 graduate courses have been stood up at AFIT through the Air Force Cyberspace Technical Center of Excellence (CyTCoE). These graduate courses are professional development courses for cyberspace professional as they transition to intermediate and higher level responsibilities. Cyber 200 and 300 courses are designed for all cyberspace professionals including the entire 17D or Cyberspace Warfare Operator career field. The courses provide an understanding of the design, development, and acquisition of cyberspace systems. They also explore cyber asset capabilities, limitations, vulnerabilities and employment in Joint military operations. The courses aim to keep cyberspace professionals current and at the cutting-edge, keeping pace with the quickly changing technologies of the cyber domain.[16]

A Cyber Weapons Instructor Course (WIC) has been launched at Nellis AFB. The U.S. Air Force Weapons School trains tactical experts and leaders of Airmen skilled in the art of integrated battle-space dominance across the land, air, space and cyber domains. Weapons Officers serve as advisors to military leaders at all levels, both those in uniform or civilian government positions. Weapons Officers are the instructors of the Air Force's instructors and the service's institutional reservoir of tactical and operational knowledge. The culmination of the course is the Advanced Integration phase in which all assets combine in challenging scenarios simulating current and future threat arenas. Students demonstrate their ability to lead and instruct while effectively integrating multiple weapons systems across the land, air, space and cyber domains.[17]

Recruitment and Retention of Reserve Component Cyberspace personnel

The nation has relied more heavily on the RCs since the end of the Cold War. Reservists have been involuntarily activated for federal service six times over the past 23 years. The RC is

an irreplaceable and cost-effective element of overall DOD capability. The RC Selected Reserve (38 percent of the total force) plays an essential, efficient, and cost-effective role in meeting the nation's strategic defense goals.

The creation of U.S. Cyber Command (USCYBERCOM)—a four-star command—and the subsequent creation of service-level three-star commands that conduct the full spectrum of operations in cyberspace have placed a new level of emphasis on those qualified to work in the evolving cyber career field. While getting a qualified work force in place has always been a challenge for the information technology (IT) community, it has been exacerbated by the emerging need to recruit, develop and retain a qualified force capable of meeting the skill requirements levied by USCYBERCOM and the DOD. USCYBERCOM has stated that it wants to develop an estimated 5,000 military and civilian personnel to make up a larger CMF to serve in three capacities: protect critical national information systems, support combatant commanders abroad and defend the DOD networks.[18]

In early 2015, U.S. Cyber Command announced that it was recruiting and training Airmen to join one the Air Force's 39 mission force team that will be established over the next two years. The command needs about 1,715 Airmen for the Air Force teams, as part of a Defense Department-wide effort that will put in place 133 CMF teams with 6,000 personnel by 2017. The mission will rely on participation from 900 RC cyber operations Airmen, who find themselves assigned to associate units that work with active-duty units, equipment and resources.[19]

DOD's Posture – The Cyber Mission Force and the Reserve Components

The creation of the Cyberspace Mission Force (CMF) in 2013 was intended to manage the Pentagon's expanding cyber workforce. The CMF has three forces, each with a specific

mission. One is the Cyber National Mission Force that defends the nation from foreign adversaries in cyberspace. Another is the Cyber Combat Mission Force that supports the services' combatant commands. Yet another is the Cyber Protection Force, which defends military networks and, when authorized, other infrastructure.[20] The cyberspace mission is unique in that, while other mission areas in the Air Force are constant or decreasing in size and scope, it is growing rapidly, similar to the rapid growth seen in the remotely piloted aircraft (RPA) mission. The RC is a key piece of the cyberspace mission, with multiple established locations and more announced or planned.[21]

Initial plans to field the CMF did not embrace RC integration. At the 5 June 2013 Reserve Forces Policy Board quarterly meeting, a Task Group led by Sergio Pecori was formalized to examine DOD's cyber approach and to provide an objective assessment of the Department's current path in developing its organizations, policies, doctrine and practices for conducting defensive and offensive cyber operations. The Task Group was further directed to comment on force mix between active, reserve, and civilian personnel and Reserve Component organization needed to meet the DOD strategy.[22] As the meeting convened, it was decided that the Reserve Components should be included in CMF requirements. The Task Group concluded that the inclusion of the RCs in CMF requirements would take advantage of reduced cost, civilian acquired skills, experience, continuity and longevity.[23]

Before this plan could be implemented, an assessment must contain a robust development of performance based metrics is required to quantify these types of future force decisions and provide a sound basis for return on investment and alternative resourcing decisions, including AC/RC force mix. The Task Group plans to reassess the CMF requirements in fiscal year (FY) 2017. Several RCs have since proposed allocating manpower and training to create Cyber

Mission Force teams; however, most are not allocated to USCYBERCOM, Combatant Commanders, or Service Cyber organizations.

DOD draws on the National Guard and Reserve Components as a resource for expertise and to foster creative solutions to cybersecurity problems. The RC offers a unique capability for supporting each of DOD's missions, including for engaging the defense industrial base and the commercial sector.[24] The Guard and Reserve provide operational forces that can be used on a regular basis, while ensuring strategic depth in the event of mid to large-scale contingencies or other unanticipated national crises when they are not being employed.[25] In addition, the advantages to using RC personnel for CMF missions is the load sharing with active duty forces, providing available surge capacity, and offering DOD trained forces to aid in the defense of national critical infrastructure if requested and authorized. The National Defense Authorization Act for Fiscal Year 2015 contained some provisions related to DOD cybersecurity and cyber operations in regards to RCs. The considerations regarded the role of RC in defense against cyberattacks given their unique experience in private and public sectors and existing relationships with local and civil authorities for emergency response.[26]

DOD's Partnership with the Public Sector in Cybersecurity Defense

DOD plans to work with the Department of Homeland Security (DHS), other interagency partners, and the private sector to improve cybersecurity. One example of such cooperation is the 2010 memorandum of agreement signed by DOD and DHS to align and enhance cybersecurity collaboration. The memorandum formalizes joint participation in program planning and improves a shared understanding of cybersecurity. Under this memorandum USCYBERCOM and DHS exchange liaison personnel. DOD supports DHS in leading interagency efforts to identify and mitigate cyberspace vulnerabilities in the nation's critical infrastructure. DOD has

the lead for the defense industrial base (DIB) sector, but will continue to support the development of whole-of-government approaches for managing risks associated with the globalization of the information and communications technology (ICT) sector.[27] DOD is partnering with the DIB to increase the safeguarding of DOD program information residing or transiting DIB unclassified networks.[28]

DHS is dramatically increasing the number of Federal civilian cyber defense teams to a total of 48 by recruiting the best cybersecurity talent across from the Federal government and private sectors. These standing teams will protect networks, systems, and data across the entire Federal Civilian Government by conducting penetration testing and proactively hunting for intruders, as well as providing incident response and security engineering expertise.[29] This initiative is in response to President Obama's Cybersecurity National Action Plan. The Obama Administration announced a series of near-term actions to enhance cybersecurity capabilities within the Federal government and across the country. But given the complexity and seriousness of the issue, the President is also asking some of our Nation's top strategic, business, and technical thinkers from outside of government to study and report on what more the U.S. can do to enhance cybersecurity awareness, protect privacy, maintain public safety as well as economic and national security, and empower Americans to take better control of their digital security.[30]

Cyberspace Defense Budget Outlook and Impact on The Reserve Components

In the Pentagon's fiscal 2011 budget proposal, cybersecurity received a $105 million increase from the previous year. The department's sub-command dedicated to cyber warfare -- a facility in Fort Meade, Md., known as U.S. Cyber Command -- is slated for a fiscal 2011 budget of $139 million under the Air Force budget proposal, in addition to funding from the U.S Strategic Command, which oversees its operations.[31]

Since 2011, the cyber training pipeline doubled in three years, big bonuses were offered to some related specialties and the U.S. Cyber Command's budget doubled to $447 million in 2014. This was in stark contrast to the looming threat of retiring entire fleets of aircraft and involuntarily separating thousands of Airmen. The Pentagon's fiscal 2014 budget requested funding for more than half a million men and women to serve in the Air Force across the Active and Reserve components, including roughly 328,000 on active duty, 105,000 in the Air National Guard and 70,000 in the Reserve.[32]

In 2014, the National Commission on the Structure of the Air Force recommended for the Air Force to change the mix of full-time and part-time personnel in the force, from the current breakdown of 69 percent active-duty Airmen and 31 percent reservists, to 58 percent active-duty Airmen and 42 percent reservists. The shift would move about 36,600 personnel into the RCs, including 22,500 into the Air National Guard and 14,100 into the Reserve. The proposal would yield savings of perhaps $2 billion per year in manpower costs with no reduction in Total Force end strength.[33]

In the FY 2015 President's Budget, the Air Force had to make tough choices and trade-offs to balance capability, capacity, and readiness. The FY 2016 President's Budget request also reflects tough choices but seeks to return the Air Force to readiness, modernization and recapitalization funding levels required to execute the defense strategy. Additionally, this budget submission is informed by current geopolitical conditions and ongoing contingency operations. It restores capacity to meet Combatant Commanders' most urgent needs, sustains readiness gains afforded by the BBA, and further invests in nuclear; space; cyber; intelligence, surveillance and reconnaissance (ISR); and command and control (C2) capabilities.[34]

The White House pitched $5.5 Billion in cyber spending for the FY 2016 budget (See Figure 2 for the budget breakdown). In 2016, the U.S. Cyber Command spending takes a 7 percent hit even as it tries to get mission troops up and rolling, according to Defense Department budget figures.[35]

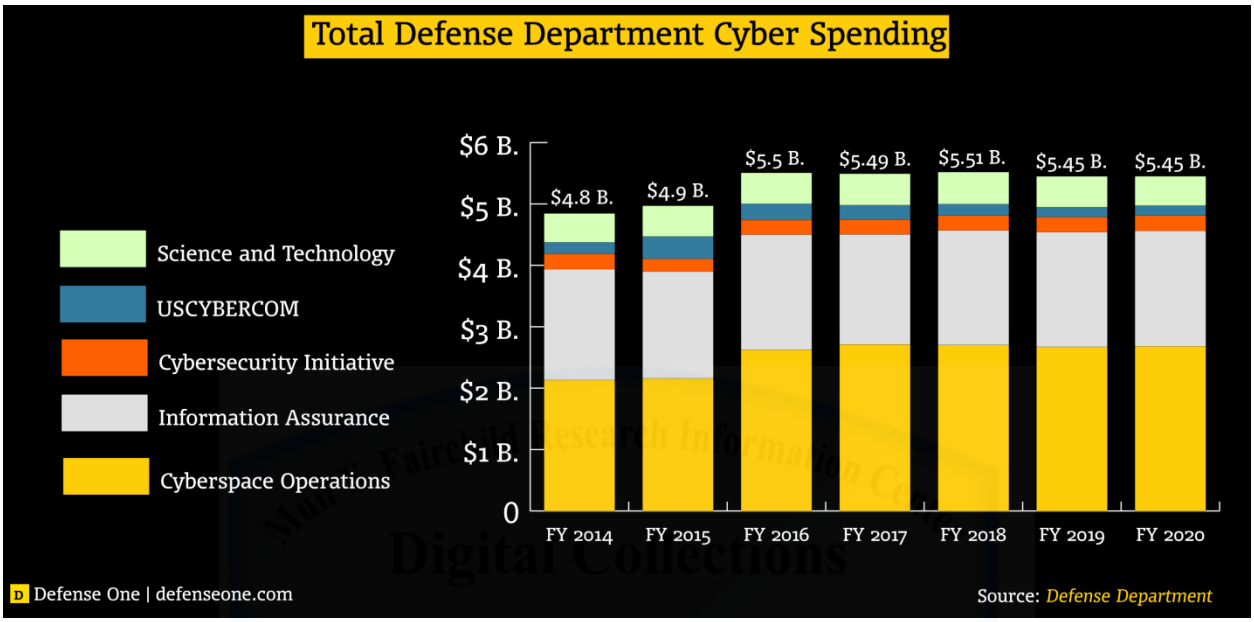

Figure 2. Total Defense Department Cyber Spending[36]

In 2014, the cyber force was funded at $546 million while 2015 projections estimated a $509 million pursue. The 2014 number included money for one-time purchases "to fit-out and lease facilities" for the cyber troops. Money for the command – tasked with orchestrating network defense maneuvers and offensive cyberattacks – will stabilize over the next five years, totaling out at $2 billion. About $500 million in 2016 would go toward compensating computer security whizzes department-wide. In the Spring of 2015, DOD received the go-ahead to fast-tract the hiring of 3,000 civilian cyber pros, in part, to staff the half-full Cyber Command.[37]

The FY 2016 funding levels achieve an appropriate balance between the Active and Reserve Components to rebalance the Joint Force for the 21st Century. The DOD's Ready

Reserve totaling about 1.1 million members costs 9 percent of the total base budget. The FY 2016 budget requested $3.1 billion for RC equipment procurement funded by the Military Services as a subset of their procurement budget. The RC and their assigned units will have access to modern equipment to train at home station, for contingency/crisis response, and to react to domestic consequence management requirements. Access to modern equipment will facilitate operational use in non-contingency missions. Fielding and support of Critical Dual Use equipment (those items that are essential for both domestic and warfighting missions) will ensure the nation's RCs can always answer the call. The FY 2016 RC budget includes $551 million for military construction to meet both current and new mission requirements for RC operations, readiness, and training facilities. The budget also funds sustainment, which is essential to maintaining facilities at a level that supports readiness and preserves the substantial investment the country has made in infrastructure.[38] The FY 2016 PB request also seeks to build and maintain a Total Force - Active, Guard and Reserve - that is both ready for the full range of military operations today and is also capable of executing its core missions against future high-end threats. The choices the Air Force makes in the budget are based upon a long-term strategy and vision, outlined by the Secretary of the Air Force and Chief of Staff of the Air Force's Call to the Future. These tough choices are informed by a realistic assessment of the fiscal and operational environment and set the conditions for the best air force for America in 2016 and beyond.

ANALYSIS

Proficiency and Readiness Training for Air Force Reserve Component Cyber Personnel

The DOD and services have recently identified gaps in regular cyber training exercises, such as Cyber Flag, which is an annual joint, interagency exercise conducted at Nellis Air Force

Base, Nevada.[39] DOD's new 2015 Cyber Strategy does not address how it's going to build and maintain ready forces in the RCs to conduct cyberspace operations.

While this paper established that Air Force RC cyber personnel are only allotted a fraction of time as compared to the AC to perform their required training (approximately 39 days per year for the average traditional Reservist), they are no less ready than their AC counterparts to support cyberspace operations. A large percentage of cyber personnel within the RCs that work in the civilian sector have the advantage of getting the necessary training outside the military channels to be proficient in their fields through their employers. In fact, RC cyber personnel who are employed by companies such as Google, Yahoo, Microsoft, and Cisco bring the most unique and current expertise.[40] Even if Air Force RC personnel do not work for those companies but work in places that implore some level of cyberspace technical expertise or utilize technologies from the above mentioned companies bring with them the most current and up-to-date technical skills.

Additional training requirements for Air Force RC personnel include compliance and readiness standards, which must be accomplished within the training year to be qualified as being ready and proficient as it affects a unit's Air and Space Expeditionary Force Unit Type Code Reporting Tool (ARTS) and Status of Resources and Training System (SORTS) reporting. Cyberspace training requirements are in addition to the training schedule making it impossible to complete the required tasks during normal operational hours. As "Citizen Airmen," there are already time constraints on the personal life juggling a military career with a demanding civilian career making it even more challenging to accomplish the Air Force's training requirements while off-duty.

The core technical training strategy for the Air Force's 23-week initial UCT could use significant improvement and revising. This initial training is seen as the basic training of military personnel in the cyber career field and provides a way for those personnel to obtain their military occupation specialty in their respective areas. The six-month UCT course spends part of its time introducing cyber officers to tactical communications, communications ethos and legality, and other traditional communications training. The rest of the time is spent trying to educate the students on cyber operations and the different skillsets.[41] The UCT is more applicable to AC personnel and other military personnel who are new to cyberspace with no prior work experience in IT related fields. Air Force RC personnel with current and prior work experience in IT related fields tend to be more knowledgeable about the UCT course content and possess current knowledge on the technologies. For Air Force RC cyber personnel, the use of this training provides them with the Air Force's operational focus on cyberspace within DOD's cyber defense posture and gives them an opportunity to apply their acquired skills to military operations within a training environment. Overall, the current training strategy does not allow enough time to cover more core skills that give hands-on experience to more technically challenging and advanced skillsets.

After initial training, cyberspace personnel are required to augment and expand on a continuous basis the knowledge and skills obtained through experience or formal education.[42] Moreover, continuing education poses a challenge for Air Force RC personnel and their units because it requires additional monetary considerations to be made outside the normal operations and maintenance and training budgets. Current statutory and funding restrictions on duties of Air Force RC personnel performing their monthly commitments limits how Air Force RCs can use this time to perform regular and recurring duties as part of an operational mission. In addition,

Air Force RCs are required to maintain specific certifications. IA certifications sometimes require renewal subscription costs and maintaining them has to be covered by the member's unit or command, or last resort by the member themselves.

Cyberspace personnel must learn a common understanding of the concepts, principles, and applications of Information Assurance (IA) for each category, specialty, level, and function to enhance protection and availability of DOD information, information systems, and networks. In order to meet these objectives, initial training through formal education at in-residence schools must be attended and IA knowledge and skills are verified through standard certification testing which must be acquired and maintained. Traditional reservists and guardsmen serving 39 days per year are not a cost-effective method for providing steady-state cyber services. If guidelines for training are adhered to, the majority of this time must be dedicated to training (perhaps not related specifically to their cyber duties), and any operational duties they perform must be incidental to their training.[43]

Personnel Recruitment and Retention in the Air Force Reserve Components

Many men and women in the U.S. Air Force are ready to answer their nation's call, to readily advance their skills, and to secure the cyberspace domain. The Air Force stands in a prime position to allow this cyber culture to develop and lead the way forward.[44] The RC has always been a vital member of the fight; the cyber domain should be no different.[45]

In keeping with the general trend, within Cyberspace operations, the Air Force Cyberspace Command (AFCYBER) – officially called 24th Air Force – has impressed upon its RCs the idea of playing a unique role in providing the DOD the additional capacity of resources (personnel and equipment) in a cyber conflict and the ability to work with the states. A large part of the Air Force's plans to increase the number of Airmen in cyberspace career fields should be

met by its RCs, which are well situated to recruit and retain from the specialized talent available in the commercial cyber labor market.[46] Air Force RC members who are employed in industries related to cyber operations can be tapped to provide current knowledge, tools, and techniques for network warfare operations.[47] This pool of expertise provides both a logical and cost-effective source for individuals with relevant advanced technology skills.

As the Air Force looks to increase its cyberspace personnel, one factor still remains to challenge these efforts – the force has to get smaller, much smaller than they have ever been. Over the next few years, the Air Force may have to reduce their force by approximately 25,000 Airmen and as many as 550 aircraft if they do not receive any budget relief.[48] The biggest challenge for the Air Force will be to ensure they keep skilled Airmen to meet the core mission requirements. Another challenge for Air Force in recruiting and retention is the military versus civilian pay compensation. The civilian sector can often offer increased compensation to attract the best and the brightest for cyber positions. However, it is difficult for the military to attract many of these same personnel because of the relatively low compensation.[49] With recent budget and personnel cuts, sequestration, higher ops tempo, and increase in deployments over the past decade, attracting and retaining highly-skilled cyberspace professionals is becoming more and more challenging.

Even though the Air Force tries to recruit and retain personnel with bachelor's degree in IT related fields to the military as well as offer incentives to attract personnel with IT work experience, the cyber-workforce shortage is a major concern and continues to be an ongoing issue. The commercial sector seems to be ahead of the power curve because of their ability to recruit for cyber rather than IT. Companies tended to actively recruit those with degrees in science, technology, engineering, and mathematics (STEM) fields, especially computer science,

InfoSec, computer engineering, and electrical engineering. While companies certainly hire from nearby regional universities, nationally known "good schools" for cyber are also valued.[50] With the civil sector offering competitive salaries to attract the best and the brightest for cyber positions, the Air Force just cannot compete with them since the military has whole tends to offer really low compensation to its members.

As the Air Force tries to bring in more manpower to support cyberspace operations without having to leverage new resources, they have considered utilizing the cross-training route for acquiring personnel from other career fields. However, only Airmen who have obtained the CompTIA Security+ certification will be considered for cross-training into cyber-related jobs. They also must have an understanding of and aptitude for TCP/IP protocols, network hardware and the Linux operating system.[51] In addition, an understanding of network fundamentals, network infrastructure, to include telecommunications theory, industrial control systems, and data communications and links are needed. Majority of the capabilities the military uses today are comprised of systems that uses very complex computer technology that has been outsourced from companies who specialize in developing these technologies. Thus, requirements for personnel with a strong technical education coupled with experience in the information technology and engineering fields become more and more essential.

Civilian Life and Military Work Balance for Reserve Component Personnel

The RCs have now become an operational force, expected to deploy at least every five years, imbuing the term "citizen soldier" with new meaning. In some cases, service members and their families will be strengthened by their experiences; other families might experience no obvious consequences now but might experience psychological or physical symptoms later in life.[52]

The Commission on the National Guard and Reserves predicted that an increasing demand for U.S. forces along with a coinciding reduction in AD end strength would cause the nation to move RC forces from a strategic reserve to an operational reserve.[53] Recent shifts in mission operations from the Air Force AC to the Air Force RCs has redefined the "weekend warrior" adage of serving just one weekend a month and two weeks a year. Many Air Force RC personnel who hold cyber responsibilities most likely carry a full-time civilian jobs due to their highly needed skillsets to fulfill the increasing requirements for cybersecurity in private sectors. This leaves them in potentially stressful circumstances, vulnerable to being deployed to a war zone in crisis while desiring to maintain their relationships with their civilian job and family responsibilities.

Sometimes, civilian employers can have trouble with even one weekend a month, especially if they require personnel to work overtime and shift work that occurs over a weekend period each month. Civilian employers may have to shift the work schedule around the Reservist's drill weekend so they can give them weekend off. If the Reservist is an IT specialist, they may get called up for extra training on new technology and this may require the weekend to get the training accomplished. On the military side, Air Force RC personnel may be called to do Reserve training two weekends in a row, dependent upon mission creep and any new emerging requirements. This leaves the individual to vacillate between the idea of whether or not it is worth the commitment to continue serving in the Air Force RCs for fear of losing a civilian job that provides for them and their families more security, stability, and higher compensation than the part-time military job.

The age in years in the Air Force RC typically range from 19 to 59 ½ years of age. This age variance pose many challenges for individuals at various stages of their lives as it relates to

personal and family commitments, and fitness requirements. Individuals can experience a great deal of family life events such as birth of children, marriages or divorces, paying for children colleges, deaths of older parents and siblings, etc. while serving in the Air Force RCs. Personnel who started their military career in the Air Force RCs at the age of 19 can serve an average of 35-40 years giving up one weekend a month and two weekends a year during this entire time. Also, depending upon contingencies that arise requiring military intervention, they can find themselves deploying multiple times during their career. Fitness requirements also pose many challenges to Air Force RC personnel's ability to keep up with the standards. Though the minimum standards change with respect to age throughout an Airman's career, developing a "fit-to-fight" physical fitness regiment requires a great deal of extra time, commitment, dedication, and management for a healthy, balanced lifestyle. Especially, since it is mostly conducted outside of a military setting. All of this has to be done in order for Air Force RC personnel to pass their required annual or bi-annual physical training test.

Operations and Training Budget for Air Force Reserve Component Missions and Personnel

The Air Force has recognized their organizational structure should be modified to best fulfill current and anticipated mission requirements in a manner consistent with available resources.[54] The modifications include greater reliance on Air National Guard (ANG) and the Air Force Reserves (AFR). While this paper outlined the tough choices that the Air Force was required to make across the force structure in order to meet budgetary limitations imposed on them, the Air Force's funding appropriations for cyberspace operations continue to see significant progress.

DOD officials state that the DOD continues to conduct analysis to determine the appropriate force structure for cyber in the Guard and Reserve components. At this time, the

Department's senior leadership has not made any decisions. However, DOD still requires Reserve forces and personnel that are trained to the highest standard, ready, and equipped with best-in-class technical capabilities to operate effectively in cyberspace. In 2013, DOD initiated a major investment in its cyber personnel and technologies by initiating the CMF. Now DOD must make good on that investment by training its people, building effective organizations and command and control systems, and fully developing the capabilities that DOD requires to operate in cyberspace.[55]

Of the $5.5 Billion that the White House pitched in cyber spending for FY 2016, the Air Force sees about $1.41 Billion which is 25.6 percent of the total budget. Figure 3 provides DOD's breakdown of FY16 IT-Cyber budget.

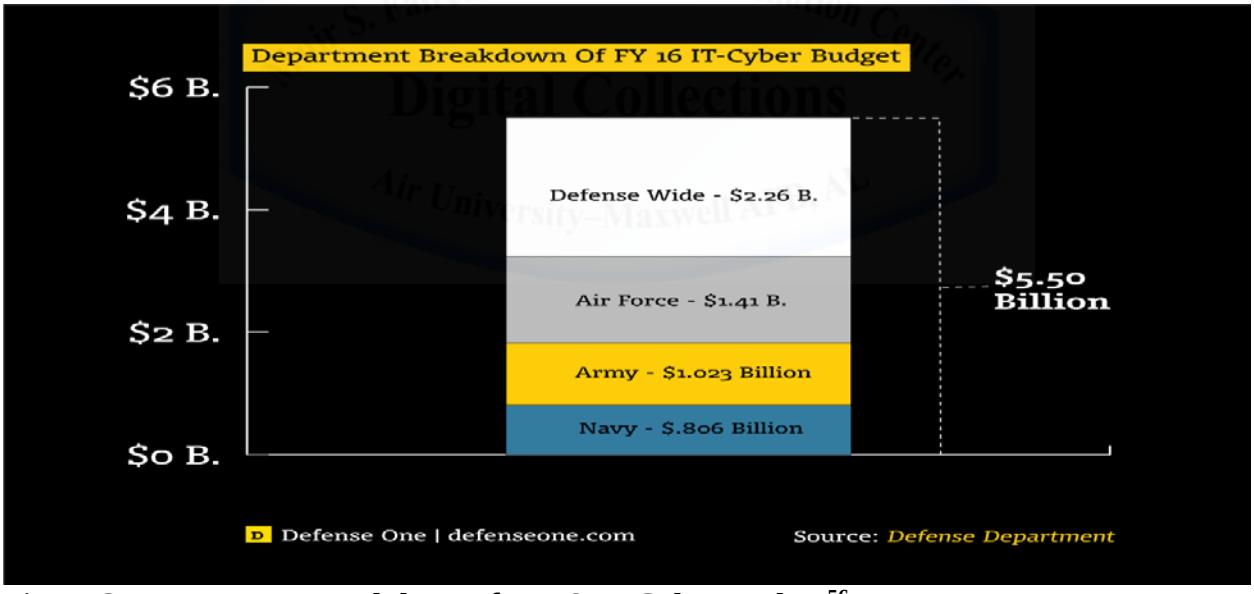

Figure 3. Department Breakdown of FY16 IT-Cyber Budget[56]

In comparison with the rest of the budget, this is only 15.5 percent less than the appropriations for defense-wide operations, and greater than 7 percent more than the Navy and Army services.

DOD's CMF personnel requirements slated for completion in 2018 is being staffed by the individual services and is expected to number more than 6,000.[57] Of that 6,000 total, the Air

Force plans to not only staff a number of those personnel but it will bolster its cyber ranks by 40 percent. For FY 2016, the Air Force saw an increase of 200 military personnel planned in cyber operations and cyber warfare positions to counter growing worldwide cyber threats.[58] The current construct of how the Air Force plans to support the cyber domain projects an overall mission force of 39 teams with 1700 personnel. It is not known yet what percentage of those teams will be staffed by RC cyber personnel to meet the operational demands.

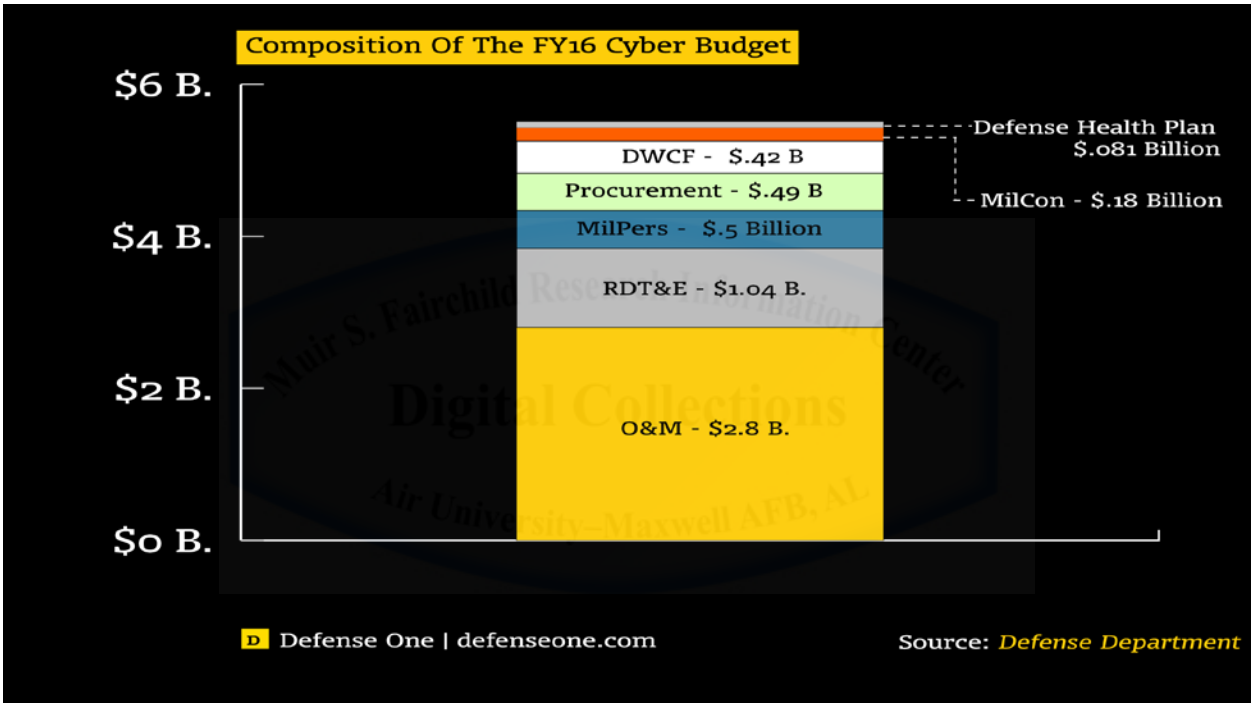

Figure 4. The Composition of the FY16 Cyber Budget[59]

Impacts of Information Technology (IT) Changes in the Cyberspace Domain

For over four decades, computer technology and the Internet have provided a strategic advantage to the United States, its citizens, and its allies.[60] Information technology (IT) offers immense capability in terms of agility, flexibility, responsiveness, and effectiveness. It enables nearly all of our military combat capability and has become a necessary element of our most critical warfare systems.[61] IT changes will have a significant impact on the cyberspace

environment not only on hardware and software equipment but also on people, activities, and data operating in and around cyberspace as well. RC cyber personnel are best suited to handle these changes. As this paper previously mentioned, many RC service members in cyberspace hold civilian jobs in advance technology fields or in providing education or training for such technologies. These personnel tend to possess most of the current knowledge, tools, and techniques obtained from industry and their civilian jobs.

Technology development and deployment will accelerate through 2025 and the nature of the threat will be continually evolving. Specific to cyberspace, in 2025, there will be a convergence of info-, nano-, and biotechnologies. The nature of devices will dramatically change, having moved from small mobile devices and augmented reality towards physical human-machine integration. The nature of secure communications and computing will have also changed with the fielding of secure quantum communication networks and small-scale quantum computers.[62]

The current defense acquisitions model may not be able to keep up with the demands of providing the U.S. military with critical warfare systems that depend on the best information technology. The conventional DOD acquisition process have been found to be too long and too cumbersome to the fit the needs of the many IT systems that require continuous changes and upgrades.[63] A unique acquisition system for IT may need to be formulated to mitigate these issues.

As changes occur in technology, DOD will have greater access to obtaining the latest and greatest technology for forces to conduct operations in the cyberspace domain. However, most of DOD's technology is outsourced and obtained from the commercial industry. This means that their adversaries also have the ability of acquiring the same technology. The nature of threats can rapidly change making it increasingly difficult for DOD to maintain the military and

technological advantage over its adversaries. RC personnel's knowledge of both the military and civil sector environments allows DOD to get a comprehensive look at all of their options before investing in equipment that may or may not provide them the advantage they were looking to obtain.

DOD's IT fiscal year budget projections to FY2020 currently shows a steady average cost ranging from $36.6 - $37 billion dollars (as shown in Figure 5). These numbers steadily climb each fiscal year as new technologies are realized and cyber threats continues to increase. The President just recently as this paper was written announced the Federal Government will need to invest additional resources in its cybersecurity. The 2017 Budget allocates more than $19 billion for cybersecurity – a more than 35 percent increase over the 2016 enacted level. The resources will enable agencies to raise their level of cybersecurity, help private sector organizations and individuals better protect themselves, disrupt and deter adversary activity, and respond more effectively to incidents.[64]

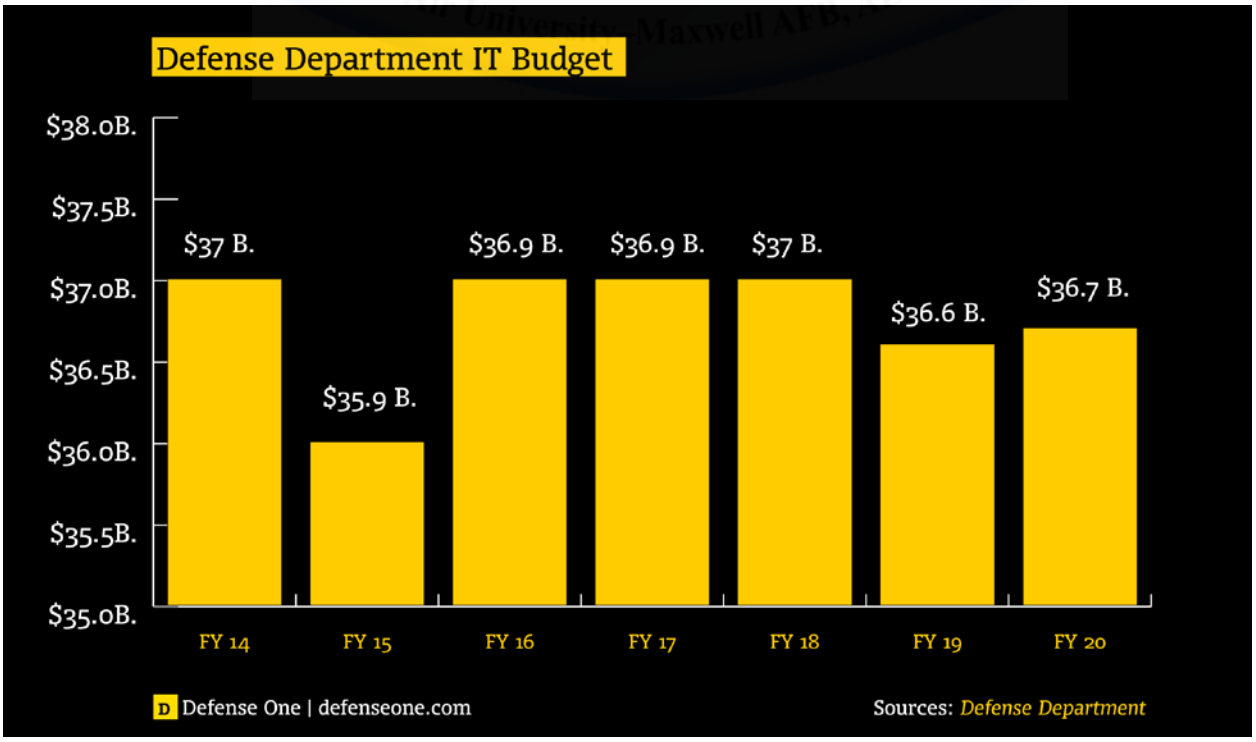

Figure 5. Defense Department IT Budget Chart

RECOMMENDATIONS

The intent of this section is to recommend strategies for the Air Force to overcome the challenges that RC personnel may face assisting DOD's initiative to achieve cyber technological dominance and military advantage over U.S. adversaries as they continue to leverage RC personnel. It will address the main concerns that the Air Force must take into consideration to recruit and retain highly qualified, skilled, and trained cyber professionals, provide the necessary training and resources to maintain the readiness and proficiency of its RC personnel, and help improve cybersecurity defense for multi-agencies across the private and public sectors. Future strategies should offer flexibility to RC personnel as they will be faced with new demands and challenges that the U.S. has never faced in its history.

Offer Incentives to Recruit and Retain Cyberspace Personnel

As mentioned earlier in this paper, the Air Force as a whole wants to bring in more manpower without having to leverage new resources. Both Guard and Reserve personnel working in cyber protection teams not only have Air Force training but also bring in their civilian expertise and experience. The Office of the Secretary of the Air Force wants to retain that investment by offering them an opportunity to come into the Air Force Reserve and continue to serve as part of the Total Force, while also pursuing their civilian career.[65]

This paper has shown that RCs are a cost-effective and irreplaceable element overall. Absorbing existing Air Force cyber personnel that are looking to leave the AC is a highly recommended approach. A significant portion of RC personnel in critical cyberspace positions had prior Active Duty experience. As the cyberspace mission continues to mature, it is expected

a similar transfer of experienced cyberspace personnel will join the RC after leaving the AC, as has historically happened in the fighter community.

However, there are major differences in compensation for Air Force cyber personnel than with fighter pilots. The Air Force offers relatively low compensation to its cyber personnel because pay is commensurate to rank rather than experience and performance. Most cyber personnel who have a sound IT background tend to make higher pay on their civilian jobs than their military rank and specialty. The Air Force simply cannot keep up with the civil sector because the pay construct is flat and consistent across the boards. It takes an act of Congress to change the military pay system for cyber personnel. In these cases, the Air Force has to become strategic and creative with incentivizing its personnel to recruit and retain the talent it expects to maintain.

To retain highly qualified cyberspace personnel, a recommendation to consider is provide incentive pay to RC cyber personnel who attains specialized skills and talent related to cyberspace. For example, when commercial airlines look at Air Force pilots, they see aviators with upward of 1,500 flying hours and 10 years or more of flying experience.[66] Commercial airlines tend to pay more for these pilots threatening the Air Force's retention efforts to keep experienced pilots in the military and in the cockpit. Moves by the Air Force to increase pilot pay, flight pay, and average basic allowance for housing tend to keep pilots serving in the Air Force longer than anticipated. Offering these types of incentives to RC cyber personnel can increase the Air Force's dividends in maintaining highly-qualified, trained IT subject matter experts.

If incentive pay is not enticing enough, the Air Force should offer critical skills retention bonuses that require an additional three to four commitment. As recent as 2014, two career

fields in Air Force cyber – 1B4X1 cyber defense operators and 1N4X1A intelligence airmen – were among just 10 specialties across the Air Force still eligible for re-enlistment bonuses. RC officers carrying the 17D Air Force specialty code designator for cyberspace operations are not eligible for such bonuses.[67] However, they tend to have higher education degrees, civilian expertise and number of years of IT-related experience, and higher paying salaries than enlisted personnel. These skills are critical for the Air Force and should not be taken likely by Air Force leaders in utilizing RC cyber personnel. This incentive will entice Airmen to stay in longer and increase their knowledge base in cyberspace operations.

Other incentives that Air Force should consider in recruiting and retaining talented individuals with a cyber background is offering retirement points for continuous learning education obtained from Air Force sponsored civilian institutions that have robust cyber training and education courses. Also, this incentive can be offered to RC cyber personnel pursuing upgrade training and certifications that can be utilized not only in the private sector but public and federal government.

Lastly, the Air Force should look at qualifying RC personnel for the post 9/11 GI bill after four years of continuous military service. The educational benefits received will push RC personnel to get additional education in areas related to cyber to further their abilities and endeavors to increase their cyber knowledge.

Allow Air Force RCs to Handle Cyberspace Support and Cyberspace Defense Missions

Many government officials suggest that Air Force RCs handling missions requiring full-time personnel to manage and support its operations may not be a viable option. Because RC personnel are only required to serve their normal 39 days a year, they are often overlooked to handle continuing missions requiring 24 hours of daily support for 365 days a year.

Traditionally, the RCs are called upon when there is a requirement for additional personnel to augment AC personnel during surge or contingencies. However, in the cyberspace arena, they are missions suitable for RC personnel to handle for the required durations. Having more cyberspace missions dedicated to the use of RC personnel running its operations may grow the cyber force and bolster an increase in the percentage of full-time personnel and the numbers of technicians and Active Guard Reservists (AGRs) in RC cyberspace units.[68]

The RC is a key piece of the cyberspace mission, with multiple established locations and more announced or planned. Figure 6 shows the bed-down of ANG Cyberspace units. RC individual mobilized augmentees (IMA) also supplement almost every cyberspace unit in the AC.[69]

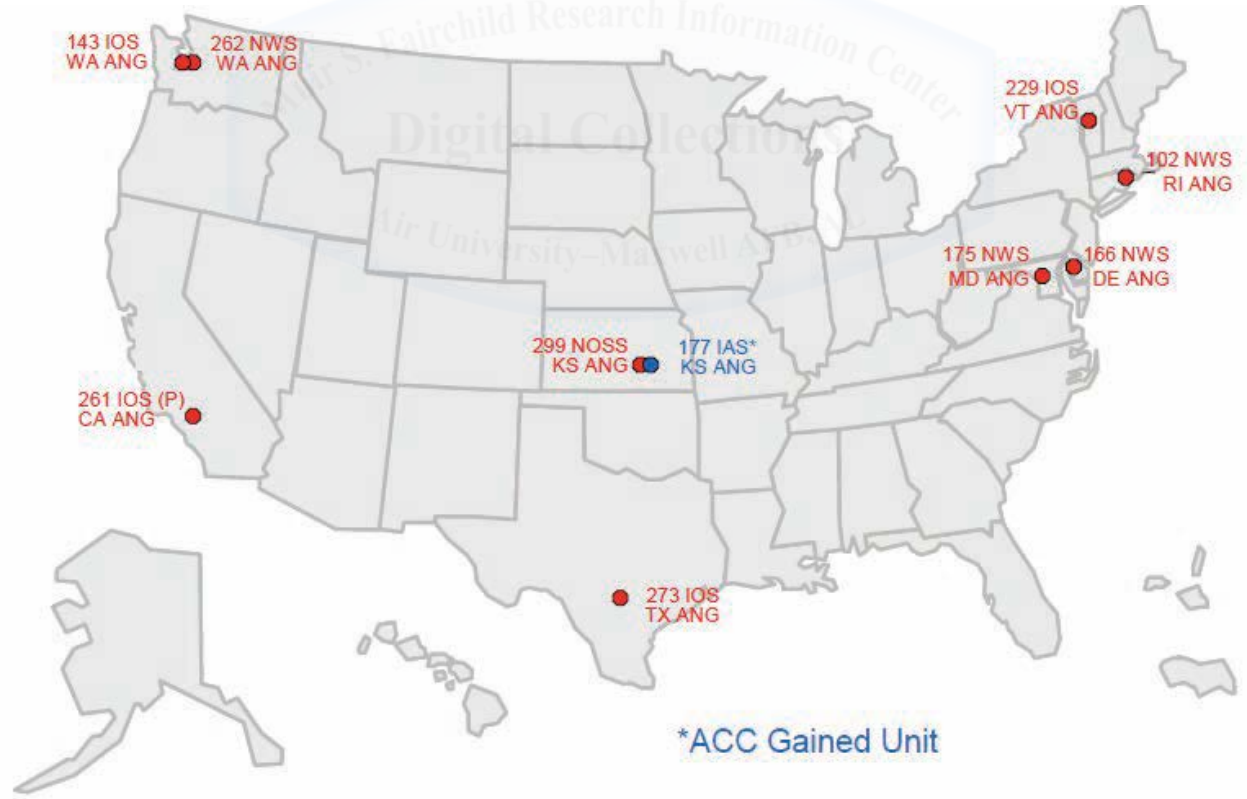

Figure 6. Air National Guard Cyberspace Units

Overall, the cyber mission has both a steady-state and a potential surge demand. Heretofore, the mission has experienced a build-up of steady state requirements. Presumably, at some point, the steady-state demand will stabilize, and surge requirements will be defined. Cyberspace support as a specific mission area does experience a surge demand during significant combat operations. Cyberspace defense does not experience a significant surge demand, though its ops tempo is high during steady-state operations. Cyberspace force application does experience a surge demand during significant combat operations. None of the three mission areas require any significant steady-state deployments. Most missions can be accomplished from any location in the United States as long as the appropriate support equipment, facilities, and connections are present.[70]

Cyberspace support and cyberspace defense mission areas have applicability to state missions. Col Tom Thomas, former commander of Delaware Air National Guard's 166th Network Warfare Squadron, noted, Protecting the networks and computer systems that are vital to a state's commerce and public safety is likely to become as much a part of the Guard's job as is stacking sand bags to keep floods from factories, hospitals and neighborhoods. The Guard stands ready to assist in deterring and responding to cyber intrusions.[71]

The Secretary of Defense has stated that the Guard and Reserve provide a critical surge capacity for cyber responders. The Air Force should continue to pursue cyberspace support and cyberspace defense missions to ensure their personnel are contributing to the cyber defense posture and are readily available anytime and anywhere to fill in the gaps of cyber mission capabilities.

Short-Duration Activations

This paper established the civilian and military work challenges Air Force RC personnel face while serving in traditional RC roles designed for service which, absent of crises, required only one weekend a month and two weeks a year. The fact remains that the U.S. has been fighting a significant conflict of some sort for at least 14 years, causing many even the most patriotic of citizens to think twice before taking on RC responsibilities. For Air Force RC cyber personnel, activations can cause even more stress and friction with their families and employers especially if it requires long durations of time away from work and family. In order for the Air Force to mitigate these issues, recommend they work to make activations for RC cyber personnel shorter than 60 days or less.

Yet such detractor to recruitment need not be the case for cyber warriors. Personnel in the cyberspace support mission area rarely require activations. Personnel in the cyberspace defense mission area may require authorization under Title 50, U.S. Code, for certain ISR activities. Personnel in the cyberspace force application mission area do require activation, per Title 10, U.S. Code, for certain activities, such as those involved in any part of a cyber "kill chain." These members of an RC unit may be on non-federal (Title 32) status when not involved with an operational mission or activity, but they must transition to Title 10 status when they participate with an operational mission or activity. Until this transitional status and associated MPA funding issues are seamless, this criterion highlights a consideration within the cyberspace enterprise.[72]

Develop Partnerships with Civilian Institutions to Incorporate Robust Cyber Training for DOD Personnel

The professional military education (PME) community could clearly benefit from the training methodologies that civilian educational institutions have established. Air Force PME for

the cyberspace career field considers cyber skills to be all the same. The education continues to fall short in its lack of specialization, functional separation, and training investment. Most colleges and universities have worked with industry to ensure their students are equipped with the latest technological theories and applications to coincide with the increasing demands for a competent workforce.

As stated earlier in this paper, due to the growing interest in cybersecurity, several large defense contractors are offering variations on their internal training curriculum to DOD. For example, Northrop Grumman offers access to its Cyber Academy; Lockheed Martin offers coursework through its Center for Security Analysis; Raytheon has a course catalog that offers everything from a three-hour cyber executive course to a 22-week cyber fundamentals course; MITRE contributes training material to OpenSecurityTraining.info; and Thales has invested in a Cyber Integration & Innovation Centre to provide cybersecurity training for clients via cyber simulator time, akin to flight simulators that pilots use to maintain currency.[73]

Most military educational institutions have the physical and technological infrastructure that can support the addition of civilian training courses to their course offerings. Recommend that the Air Force adopt a similar training methodology by investing in civilian instructors to teach at military education institutes who possess the knowledge and aptitude to keep up with industry standards. The curriculum should be modeled after institutions that offer cyber technology degrees but tailored to meet the Air Force training requirements for military cyber defense. In addition, the Air Force should offer cyber degrees for its personnel who are required to complete PME for professional development. By implementing these recommendations, the Air Force and DOD would increase its breadth in cyber knowledge and a growing interest from its personnel pursuing cyberspace technical degrees.

Incentivize Civilian Employers of Reserve Component Cyber Personnel

This paper discussed the potential issues that RC cyber personnel faces with civilian employers while maintaining their service commitment. As a way to mitigate issues when Air Force RC cyber personnel are activated to support military operational and contingency plans, incentives should go to civilian employers such as additional tax breaks In addition, the government should incentivize companies with monetary support if they offer differential pay to its employees if they suffer a loss in pay while activated. Although, RC personnel are protected by the Uniformed Services Employment and Reemployment Right Act of 1994 (USERRA) is a federal law that establishes rights and responsibilities for uniformed service members and their civilian employers.[74] This law does not guarantee the uniformed service maintain their jobs after reinstatement. By offering additional incentives to employers of RC cyber personnel, this will increase their desire to hire more personnel that serve and help the Air Force and DOD retain cyber personnel who are willing to stay in the RCs.

CONCLUSION

Leaders from the ANG and AFR ultimately have the responsibility of ensuring their Airmen are ready and proficient to meet any and all mission requirements within DOD. ANG and AFR leaders should collectively send a clear message to DOD that the RCs are the linchpin to meeting operational demands for cyber offensive cyberspace operations (OCO) and defensive cyberspace operations (DCO). However, they must do so by strategizing and quantifying the appropriate resources for the RC end-strength.

The current traditional training construct of 39 days a year clearly does not provide enough time during normal duty hours of operation for RC personnel to avail themselves fully to proficiency training in military cyber defense. However, military employers and civilian

workplaces can play a major part in reducing or exacerbating the challenges RC personnel face with their Reserve commitments.

Given the 'extreme work' these service members and their families volunteered to perform on behalf of this country, it is reasonable to consider the need for 'extreme work-family' support in return.[75] If this problem is not addressed properly, there is a high probability that the RCs may see a major decline in the participation and support of an American patriotic society in favor of an all-volunteer force with citizen soldiers augmenting the shortfalls in Active Duty personnel. Empowering RCs to formulate changes necessary to provide DOD with what is best for the RCs supporting the cyber mission is fundamental.

NOTES

[1] Lyngaas, Sean, *"Guard, Reserve are X Factors in Cyber Plans,"* The Business of Federal Technology, https://fcw.com/articles/2015/05/07/guard-reserve-cyber-plans.aspx, May 07, 2015
[2] *Cybersecurity National Action Plan Fact Sheet,* https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan, 09 February 2016
[3] Cyberspace Operations, Joint Publication 3-12(R), 5 February 2013, p.I-8
[4] *What is Cyber Security?* https://www.paloaltonetworks.com/resources/learning-center/what-is-cyber-security.html
[5] "The Department of Defense Cyber Strategy," http://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy
[6] Cyberspace Operations, Joint Publication 3-12(R), 5 February 2013, p.I-2
[7] Ibid, I-3
[8] Ibid, I-3
[9] Ibid, I-3
[10] Ibid, I-4
[11] Welsh, William, "*Cyber Warriors: The Next Generation,"* Defense Systems, https://defensesystems.com/articles/2014/01/23/next-generation-cyber-warriors.aspx, January 23, 2014
[12] Pawlyk, Oriana, "*Cyber: The Safest Job In The Air Force,"* Military Times, http://www.militarytimes.com/story/military/archives/2014/02/20/cyber-the-safest-job-in-the-air-force-/78543786/, February 20, 2014
[13] Ibid
[14] Ibid
[15] Ibid
[16] 88th Air Base Wing Public Affairs, *"Air Force Launches Advanced Cyberspace Courses,"* http://www.afspc.af.mil/news/story.asp?id=123225585, October 7, 2010
[17] United States Air Force Weapons School Factsheet, http://www.nellis.af.mil/library/factsheets/, Aug 12, 2015

[18] Quick, Christopher R., *"Creating a Total Army Cyber Force: How to Integrate the Reserve Component into the Cyber Fight,"* The Land Warfare Papers No. 103W, September 2014, p.1
[19] Pawlyk, Oriana, "Calling up the Reserves: Cyber mission is recruiting" Air Force Times http://www.airforcetimes.com/story/military/careers/air-force/2015/01/03/us-cyber-command-recruiting/21226161/
[20] Welsh, William, "*Cyber Warriors: The Next Generation,"* Defense Systems, https://defensesystems.com/articles/2014/01/23/next-generation-cyber-warriors.aspx, January 23, 2014
[21] Albert A. Robbert, James H. Bigelow, John E. Boon, Jr., Lisa M. Harrington, Michael McGee, S. Craig Moore, Daniel M. Norton, William W. Taylor, "*Suitability of Missions for the Air Force Reserve Components,"* RAND Project Air Force, 2014, p.58
[22] Reserve Forces Policy Board, "Department of Defense Cyber Approach: Use of the National Guard and Reserve in the Cyber Mission Force," Report to the Secretary of Defense, RFPB Report FY14-03, 18 August 2014, p.3
[23] Ibid, p.3
[24] The Department of Defense Cyber Strategy, April 2015, p. 18
[25] Office of the Vice Chairman of the Joint Chiefs of Staff and Office of Assistant Secretary Defense for Reserve Affairs, "Comprehensive Review of the Future Role of the Reserve Component," Vol. I, Executive Summary & Main Report, 5 April 2011, p.4
[26] Theohary, Catherine A., and Harrington, Anne I., "Cyber Operations in DOD Policy and Plans: Issues for Congress," 5 January 2015, p.29
[27] Cyberspace Operations, Joint Publication 3-12(R), 5 February 2013, p.I-8
[28] Ibid, I-8
[29] *Cybersecurity National Action Plan Fact Sheet,* https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan, 09 February 2016
[30] Ibid
[31] Kruzel, John J., "Cybersecurity Seizes More Attention, Budget Dollars," American Forces Press Service, U.S. Department of Defense, 4 Feb 2010
[32] McGarry, Bendan, "Panel to Air Force: Send Airmen to the Reserve," http://www.military.com/daily-news/2014/01/31/panel-to-air-force-send-Airmen-to-the-reserve.html, 31 January 2014
[33] National Commission on the Structure of the Air Force's Report Recommends Force Structure Shift, Greater Integration, http://afcommission.whs.mil/index.php/activities/jaunary-30-2014, 30 January 2014,
[34] *Fiscal Year 2017 Air Force Budget Materials,* Air Force Financial Management & Comptroller, http://www.saffm.hq.af.mil/budget/
[35] Sternstein, Aliya, *"The Military's Cybersecurity Budget in 4 Charts,"* Defense One, *h*ttp://www.defenseone.com/management/2015/03/militarys-cybersecurity-budget-4-charts/107679/, March 16, 2015
[36] Ibid
[37] Ibid
[38] Office of the Under Secretary of Defense (Comptroller) Chief Financial Officer, "United States Department of Defense Fiscal Year 2016 Budget Request Overview," February 2015, pp. 5-5–5-8
[39] Welsh, William, "*Cyber Warriors: The Next Generation,"* Defense Systems, https://defensesystems.com/articles/2014/01/23/next-generation-cyber-warriors.aspx, January 23, 2014
[40] Albert A. Robbert, James H. Bigelow, John E. Boon, Jr., Lisa M. Harrington, Michael McGee, S. Craig Moore, Daniel M. Norton, William W. Taylor, "*Suitability of Missions for the Air Force Reserve Components,"* RAND Project Air Force, 2014, p.60
[41] Lee, 1st Lt Robert M., "The Failing Of Air Force Cyber," 1 November 2013, http://www.afcea.org/content/?q=failing-air-force-cyber
[42] DOD 8570.01-M, Information Assurance Workforce Improvement Program, Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer, December 19, 2005, Incorporation Change 3, January 24, 2012, p.12
[43] Albert A. Robbert, James H. Bigelow, John E. Boon, Jr., Lisa M. Harrington, Michael McGee, S. Craig Moore, Daniel M. Norton, William W. Taylor, "*Suitability of Missions for the Air Force Reserve Components,"* RAND Project Air Force, 2014, p.61

[44] Lee, 1st Lt Robert M., “The Failing Of Air Force Cyber,” 1 November 2013,

http://www.afcea.org/content/?q=failing-air-force-cyber

[45] Quick, Christopher R., *"Creating a Total Army Cyber Force: How to Integrate the Reserve Component into the Cyber Fight,"* The Land Warfare Papers No. 103W, September 2014, p.2

[46] McGarry, Brendon, "*Panel to Air Force: Send Airmen to the Reserve,"* http://www.military.com/daily-news/2014/01/31/panel-to-air-force-send-airmen-to-the-reserve.html, 31 January 2014

[47] Albert A. Robbert, James H. Bigelow, John E. Boon, Jr., Lisa M. Harrington, Michael McGee, S. Craig Moore, Daniel M. Norton, William W. Taylor, "*Suitability of Missions for the Air Force Reserve Components,"* RAND Project Air Force, 2014, p.62

[48] Svan, Jennifer H., "*Air Force Announces More Force Reductions,"* Stars and Stripes, http://www.stripes.com/news/air-force-announces-more-force-reductions-1.257164, 12 December 2013

[49] Albert A. Robbert, James H. Bigelow, John E. Boon, Jr., Lisa M. Harrington, Michael McGee, S. Craig Moore, Daniel M. Norton, William W. Taylor, "*Suitability of Missions for the Air Force Reserve Components,"* RAND Project Air Force, 2014, p.62

[50] Lara Schmidt, Caolionn O'Connell, Hirokazu Miyake, Akhil R. Shah, Joshua William Baron, Geof Nieboer, Rose Jourdan, David Senty, Zev Winkelman, Louise Taggart, Susanne Sondergaard, Neil Robinson, "*Cyber Practices: what Can The U.S. Air Force Learn from the Commercial Sector?", RAND Corporation, 2015,* p.47

[51] Pawlyk, Oriana, "*Cyber: The Safest Job In The Air Force,"* Military Times, http://www.militarytimes.com/story/military/archives/2014/02/20/cyber-the-safest-job-in-the-air-force-/78543786/, February 20, 2014

[52]Wadsworth, Shelley MacDermid, and Southwell, Kenona, "*Military Families: Extreme Work and Extreme 'Work-Family'",* Military Family Research Institute at Purdue University, 30 November 2010, p.14

[53]Murray, LTC Wesley D., "How to Maintain an Operational Reserve?: Further Engaging Army Reserve Components in the Coming Decade," Air War College, Air University, 17 February 2015, p.11

[54] National Commission on the Structure of the Air Force's Report Recommends Force Structure Shift, Greater Integration, http://afcommission.whs.mil/index.php/activities/jaunary-30-2014, 30 January 2014

[55] The Department of Defense Cyber Strategy, April 2015, p. 13

[56] Sternstein, Aliya, *"The Military's Cybersecurity Budget in 4 Charts,"* Defense One, *h*ttp://www.defenseone.com/management/2015/03/militarys-cybersecurity-budget-4-charts/107679/, March 16, 2015

[57] Pomerleau, Mark, "*Air Force Bolsters Its Cyber Ranks by 40 Percent,"* Cyber Defense, https://defensesystems.com/articles/2016/01/04/air-force-boosts-cyber-ranks.aspx, January 04, 2016

[58] *United States Air Force Fiscal Year 2016 Budget Overview,* February 2015, p.CM9

[59] Sternstein, Aliya, *"The Military's Cybersecurity Budget in 4 Charts,"* Defense One, *h*ttp://www.defenseone.com/management/2015/03/militarys-cybersecurity-budget-4-charts/107679/, March 16, 2015

[60] *Cybersecurity National Action Plan Fact Sheet,* https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan, 09 February 2016

[61] *Department of Defense Policies and Procedures For The Acquisition of Information Technology, March 2009,* p.vii, Executive Summary

[62] "Cyber Vision 2025". *United States Air Force Cyberspace Science and Technology Vision 2012-2025*, AF/ST TR 12-01, 13 December 2012, p.13

[63] *Department of Defense Policies and Procedures For The Acquisition of Information Technology, March 2009,* p.5

[64] *Cybersecurity National Action Plan Fact Sheet,* https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan, 09 February 2016

[65] Pawlyk, Oriana, *"Calling Up The Reserves: Cyber Mission Is Recruiting,"* The Air Force Times, 5 January 2015

[66] http://www.airforcetimes.com/story/military/2015/04/20/airlines-increase-pilot-hiring-threaten-af-retention/25941529/

[67] Pawlyk, Oriana, "*Cyber: The Safest Job In The Air Force,"* Military Times, http://www.militarytimes.com/story/military/archives/2014/02/20/cyber-the-safest-job-in-the-air-force-/78543786/, February 20, 2014

[68] Albert A. Robbert, James H. Bigelow, John E. Boon, Jr., Lisa M. Harrington, Michael McGee, S. Craig Moore, Daniel M. Norton, William W. Taylor, "*Suitability of Missions for the Air Force Reserve Components,"* RAND Project Air Force, 2014, p.60

[69] Ibid, 58
[70] Ibid, 59
[71] Ibid, 62
[72] Ibid, 60
[73] Lara Schmidt, Caolionn O'Connell, Hirokazu Miyake, Akhil R. Shah, Joshua William Baron, Geof Nieboer, Rose Jourdan, David Senty, Zev Winkelman, Louise Taggart, Susanne Sondergaard, Neil Robinson, "*Cyber Practices: What Can The U.S. Air Force Learn from the Commercial Sector?", RAND Corporation, 2015,* p.18
[74] http://www.esgr.mil/USERRA/What-is-USERRA.aspx
[75] Wadsworth, Shelley MacDermid, and Southwell, Kenona, "*Military Families: Extreme Work and Extreme 'Work-Family'",* Military Family Research Institute at Purdue University, 30 November 2010, p.14

BIBLIOGRAPHY

88th Air Base Wing Public Affairs, *"Air Force Launches Advanced Cyberspace Courses,"* http://www.afspc.af.mil/news/story.asp?id=123225585, October 7, 2010.

Applegate, LTC Scott D., *"Leveraging Cyber Militias as a Force Multiplier in Cyber Operations,"* Center for Secure Information Systems, George Mason University, 2012.

Cyber Mission Analysis: Mission Analysis for Cyber Operations of Department of Defense, Submitted in compliance with the reporting requirement contained in the Fiscal Year 2014 National Defense Authorization Act section 933(d), Public Law 113-66, 21 August 2014.

Cybersecurity National Action Plan Fact Sheet, https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan, 09 February 2016.

Cyberspace Operations, Joint Publication 3-12(R), 5 February 2013.

"Cyber Vision 2025". *United States Air Force Cyberspace Science and Technology Vision 2012-2025*, AF/ST TR 12-01, 13 December 2012.

Dale, Catherine (Specialist in International Security), "The 2014 Quadrennial Defense Review (QDR) and Defense Strategy: Issues for Congress," 24 February 2014.

Department of Defense Cyberspace Workforce Strategy (DCWS) (4 December 2013).

The Department of Defense Cyber Strategy, April 2015.

Department of Defense Policies and Procedures For The Acquisition of Information Technology, March 2009.

Department of The Air Force, "AFSC 17X Cyberspace Operations Officer: Career Field Education And Training Plan", 01 June 2015.

DOD 8570.01-M, Information Assurance Workforce Improvement Program, Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer, December 19, 2005, Incorporation Change 3, January 24, 2012.

Fiscal Year 2017 Air Force Budget Materials, Air Force Financial Management & Comptroller, http://www.saffm.hq.af.mil/budget/

Kruzel, John J., "Cybersecurity Seizes More Attention, Budget Dollars," American Forces Press Service, U.S. Department of Defense, 4 Feb 2010.

Lara Schmidt, Caolionn O'Connell, Hirokazu Miyake, Akhil R. Shah, Joshua William Baron, Geof Nieboer, Rose Jourdan, David Senty, Zev Winkelman, Louise Taggart, Susanne Sondergaard, Neil Robinson, "*Cyber Practices: What Can The U.S. Air Force Learn from the Commercial Sector?"* RAND Corporation, 2015.

Lee, 1st Lt Robert M., "The Failing Of Air Force Cyber," http://www.afcea.org/content/?q=failing-air-force-cyber, 1 November 2013.

Lyngaas, Sean, *"Guard, Reserve are X Factors in Cyber Plans,"* The Business of Federal Technology, https://fcw.com/articles/2015/05/07/guard-reserve-cyber-plans.aspx, May 07, 2015.

McGarry, Bendan, "Panel to Air Force: Send Airmen to the Reserve," http://www.military.com/daily-news/2014/01/31/panel-to-air-force-send-Airmen-to-the-reserve.html, 31 January 2014.

Murray, LTC Wesley D., "How to Maintain an Operational Reserve?: Further Engaging Army Reserve Components in the Coming Decade," Air War College, Air University, 17 February 2015.

National Commission on the Structure of the Air Force's Report Recommends Force Structure Shift, Greater Integration, http://afcommission.whs.mil/index.php/activities/jaunary-30-2014, 30 January 2014

Office of the Under Secretary of Defense (Comptroller) Chief Financial Officer, "United States Department of Defense Fiscal Year 2016 Budget Request Overview," February 2015.

Office of the Vice Chairman of the Joint Chiefs of Staff and Office of Assistant Secretary Defense for Reserve Affairs, "Comprehensive Review of the Future Role of the Reserve Component," Vol. I, Executive Summary & Main Report, 5 April 2011.

Pawlyk, Oriana, *"Calling Up The Reserves: Cyber Mission Is Recruiting,"* The Air Force Times, 5 January 2015.

Pawlyk, Oriana, "*Cyber: The Safest Job In The Air Force,"* Military Times, http://www.militarytimes.com/story/military/archives/2014/02/20/cyber-the-safest-job-in-the-air-force-/78543786/, February 20, 2014.

Pomerleau, Mark, "*Air Force Bolsters Its Cyber Ranks by 40 Percent,"* Cyber Defense, https://defensesystems.com/articles/2016/01/04/air-force-boosts-cyber-ranks.aspx, January 04, 2016.

Quick, Christopher R., *"Creating a Total Army Cyber Force: How to Integrate the Reserve Component into the Cyber Fight,"* The Land Warfare Papers No. 103W, September 2014.

Reserve Forces Policy Board, Department of Defense Cyber Approach: Use of the National Guard and in the Cyber Mission Force, Report to the Secretary of Defense, 18 August 2014.

Robbert, Albert A., Bigelow, James H., Boon, John E., Jr., Harrington, Lisa M., McGee, Michael, Moore, S. Craig, Norton, Daniel M., Taylor, William W., *"Suitability of Missions for the Air Force Reserve Components,"* RAND Project Air Force, 2014.

Sternstein, Aliya, *"The Military's Cybersecurity Budget in 4 Charts,"* Defense One, *h*ttp://www.defenseone.com/management/2015/03/militarys-cybersecurity-budget-4-charts/107679/, March 16, 2015.

Svan, Jennifer H., "Air Force Announces More Force Reductions," Stars and Stripes, http://www.stripes.com/news/air-force-announces-more-force-reductions-1.257164, 12 December 2013.

Theohary, Catherine A., and Harrington, Anne I., "Cyber Operations in DOD Policy and Plans: Issues for Congress," 5 January 2015.

United States Air Force Fiscal Year 2016 Budget Overview, February 2015.

United States Air Force Weapons School Factsheet, http://www.nellis.af.mil/library/factsheets/, Aug 12, 2015.

U.S. Department of Homeland Security, Homeland Security Advisory Council, CyberSkills Task Force Report, Fall 2012.

Wadsworth, Shelley MacDermid, and Southwell, Kenona, *"Military Families: Extreme Work and Extreme 'Work-Family'"*, Military Family Research Institute at Purdue University, 30 November 2010.

Welsh, William, *"Cyber Warriors: The Next Generation,"* Defense Systems, https://defensesystems.com/articles/2014/01/23/next-generation-cyber-warriors.aspx, January 23, 2014.

What is Cyber Security? https://www.paloaltonetworks.com/resources/learning-center/what-is-cyber-security.html